ELSEVIER

Available online at www.sciencedirect.com

SCIENCE DIRECT®

Discrete Applied Mathematics 128 (2003) 157–164

DISCRETE APPLIED MATHEMATICS

www.elsevier.com/locate/dam

On equidistant constant weight codes

Fang-Wei Fu[a,1], Torleiv Kløve[b,*,2], Yuan Luo[c], Victor K. Wei[b]

[a] *Temasek Laboratories, National University of Singapore, 10 Kent Ridge Crescent, Singapore 119260*

[b] *Department of Information Engineering, The Chinese University of Hong Kong, Shatin, NT, Hong Kong*

[c] *Institut für Experimentelle Mathematik, Universität Gesamthochschule Essen, Ellernstraße 29, 45326 Essen, Germany*

Received 26 February 2001; received in revised form 11 October 2001; accepted 8 April 2002

Abstract

Equidistant constant weight codes are studied in this paper. The dual distance distribution of equidistant constant weight codes is investigated and used to obtain upper bounds on the size of such codes as well as equidistant codes in general.

Keywords: Equidistant constant weight codes; Equidistant codes; Distance enumerator; MacWilliams–Delsarte identity

1. Introduction

Binary constant weight codes have been extensively studied by many authors. For a good survey paper, see Brouwer et al. [1]. Recently, there have been several papers dealing with non-binary CWC. For some references, see [13]. Equidistant codes have also been studied by a number of authors, mainly as examples of designs and other combinatorial objects. Some references are [3,7,8,10,11,14,16].

A few papers study codes which are both equidistant and of constant weight, for example [9,12]. Such codes are the topic of this paper.

* Corresponding author. Present address: Department of Computer Science, Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong.

E-mail addresses: tslfufw@nus.edu.sg (Fang-Wei Fu), tklove@cs.ust.hk (Torleiv Kløve), yluo@exp-math.uni-essen.de (Yuan Luo), kwwei@ie.cuhk.edu.hk (Victor K. Wei).

[1] On leave from the Department of Mathematics, Nankai University, Tianjin 300071, China.

[2] On leave from University of Bergen, Norway.

0166-218X/03/$ - see front matter
PII: S0166-218X(02)00442-0

2. Some notations and a basic relation

Consider a finite set with q elements and containing a distinguished element ("zero"). The choice of set does not matter in our context and we will use the set Z_q of integers modulo q. Let $V_n(q)$ be the set of n-tuples (or vectors) over Z_q.

Let $d_H(a,b)$ denote the Hamming distance between the vectors a and b, and $w_H(a)$ denote the Hamming weight of the vector a. Let $V_{n,w}(q)$ be the set of n-tuples over Z_q of Hamming weight w.

A code is called constant weight if all the code words have the same weight. A code is called equidistant if all the distances between distinct code words are the same. Let $B_q(n,d)$ denote the maximum number M of code words in an equidistant code over Z_q with length n and distance d (called an $(n,M,d;q)$ equidistant code) and $B_q(n,d,w)$ denote the maximum number M of code words in an equidistant constant weight code over Z_q with length n, distance d, and weight w (called an $(n,M,d,w;q)$ equidistant constant weight code).

These are closely related as shown by the following theorem:

Theorem 1.

$$B_q(n,d) = 1 + B_q(n,d,d).$$

Proof. If C is an $(n,M,d,d;q)$ equidistant constant weight code, then $C \cup \{\mathbf{0}\}$ is an $(n,M+1,d;q)$ equidistant code. If C is an $(n,M,d;q)$ equidistant code, then for every $c \in C$, the code $\{c' - c \mid c' \in C, c' \neq c\}$ is an $(n,M-1,d,d;q)$ equidistant constant weight code. □

3. Upper bounds

A general result by Delsarte [2] implies that

$$B_q(n,d) \leqslant (q-1)n + 1. \tag{1}$$

Below we shall give a series of upper bounds which under some conditions improve (1). Let C be a q-ary code of length n and size M. The distance distribution of C is defined by

$$D_i = \frac{1}{M}|\{(a,b) \mid a,b \in C, d_H(a,b) = i\}|, \quad i = 0,1,\ldots,n.$$

In particular, if C is equidistant with distance d, then

$$D_0 = 1, \quad D_d = M-1, \quad D_i = 0 \quad \text{otherwise.} \tag{2}$$

Let ξ be a primitive qth root of unity in the set of complex numbers. The dual distance distribution of the code C is defined as

$$\hat{D}_k = \frac{1}{M^2} \sum_{u \in V_{n,k}(q)} \left| \sum_{c \in C} \xi^{\langle u,c \rangle} \right|^2, \quad k = 0,1,\ldots,n, \tag{3}$$

where $\langle x, y\rangle = x_1y_1 + \cdots + x_ny_n$, the scalar product of the vectors $x = (x_1, x_2, \ldots, x_n)$, $y = (y_1, y_2, \ldots, y_n) \in V_n(q)$.

The MacWilliams–Delsarte identity gives the following relationship between the distance distribution and the dual distance distribution:

$$\hat{D}_k = \frac{1}{M}\sum_{i=0}^{n} P_k(i)D_i, \quad k = 0, 1, \ldots, n. \tag{4}$$

Here $P_k(i)$ is the Krawtchouk polynomial defined by

$$P_k(i) = \sum_{j=0}^{k} \binom{i}{j}\binom{n-i}{k-j}(-1)^j(q-1)^{k-j}.$$

Note that $P_0(i) = 1$ for all i, and

$$P_k(0) = \binom{n}{k}(q-1)^k = |V_{n,k}(q)|. \tag{5}$$

Also, it is well known that

$$P_k(0) \geqslant P_k(i) \quad \text{for all } i, k \in \{0, 1, 2, \ldots, n\}. \tag{6}$$

We include the simple proof. By the Vandermonde convolution formula

$$\binom{n}{k} = \sum_{j=0}^{k} \binom{i}{j}\binom{n-i}{k-j}$$

and so

$$P_k(0) - P_k(i) = \sum_{j=0}^{k} \binom{i}{j}\binom{n-i}{k-j}(q-1)^{k-j}((q-1)^j - (-1)^j) \geqslant 0.$$

If C is an $(n, M, d; q)$ equidistant code, then (4) implies that

$$\hat{D}_k = \frac{1}{M}\{P_k(0) + (M-1)P_k(d)\}, \quad k = 0, 1, \ldots, n.$$

Hence we get the following lemma:

Lemma 1. *Let C be an equidistant $(n, M, d; q)$ code. Then*

$$M(\hat{D}_k - P_k(d)) = P_k(0) - P_k(d) \tag{7}$$

for $k = 0, 1, \ldots, n$.

We next give a bound on $\hat{D}_k$ for constant weight codes.

Lemma 2. *Let C be a constant weight code over Z_q with length n, size M and weight w. Then*

$$\hat{D}_k \geqslant \frac{P_k(w)^2}{P_k(0)} \tag{8}$$

for $k = 0, 1, \ldots, n$.

Proof. From (3) and the Cauchy inequality ($\sum_{i=1}^{N}|a_i|^2 \geqslant 1/N\,|\sum_{i=1}^{N} a_i|^2$), we have

$$\hat{D}_k \geqslant \frac{1}{M^2}\frac{1}{|V_{n,k}(q)|}\left|\sum_{u\in V_{n,k}(q)}\sum_{c\in C}\xi^{\langle u,c\rangle}\right|^2. \tag{9}$$

Since for every $c\in C$, $w_{\mathrm{H}}(c)=w$, we know from [15, Lemma 5.3.1] that

$$\sum_{u\in V_{n,k}(q)}\xi^{\langle u,c\rangle} = P_k(w)$$

and so

$$\sum_{u\in V_{n,k}(q)}\sum_{c\in C}\xi^{\langle u,c\rangle} = \sum_{c\in C}\sum_{u\in V_{n,k}(q)}\xi^{\langle u,c\rangle} = MP_k(w). \tag{10}$$

Combining (5), (9) and (10) yields (8). This completes the proof of Lemma 2. □

We note that for $1\leqslant k\leqslant n$, relations (6) and (7) imply that $\hat{D}_k - P_k(d)\geqslant 0$. Further, if u is some real number such that $P_k(d)<u\leqslant \hat{D}_k$, then (7) implies that $M\leqslant (P_k(0)-P_k(d))/(u-P_k(d))$. In particular, from (8) we get the following theorem:

Theorem 2. *If* $k\in\{1,2,\ldots,n\}$ *and*

$$P_k(w)^2 > P_k(d)P_k(0), \tag{11}$$

then

$$B_q(n,d,w)\leqslant \frac{P_k(0)^2 - P_k(d)P_k(0)}{P_k(w)^2 - P_k(d)P_k(0)}.$$

Combining Theorems 1 and 2, we get the following bound:

Theorem 3. *If* $k\in\{1,2,\ldots,n\}$ *and*

$$P_k(d) < 0, \tag{12}$$

then

$$B_q(n,d)\leqslant 1-\frac{P_k(0)}{P_k(d)}.$$

Depending on the parameters n,q,d,w, conditions (11) and (12) will typically be satisfied for some values of k and not for others.

4. Some special cases

For $k=1$, Theorem 2 gives the known generalized Johnson bound [4]:

Corollary 1. *If* $qw^2 - 2(q-1)nw + n(q-1)d > 0$, *then*

$$B_q(n,d,w) \leqslant \frac{n(q-1)d}{qw^2 - 2(q-1)nw + n(q-1)d}.$$

Similarly, $k = 1$ in Theorem 3 gives the Plotkin bound:

Corollary 2. *If* $qd - n(q-1) > 0$, *then*

$$B_q(n,d) \leqslant \frac{qd}{qd - n(q-1)}.$$

Note that

$$\text{if } qd - n(q-1) = 1 \quad \text{then } \frac{qd}{qd - n(q-1)} = (q-1)n + 1$$

and

$$\text{if } qd - n(q-1) > 1 \quad \text{then } \frac{qd}{qd - n(q-1)} < (q-1)n + 1,$$

that is, when it applies, the Plotkin bound is at least as good as bound (1) by Delsarte.

For $k \geqslant 2$ we get new bounds. For example, for $k = 2$ we get the following bounds in Theorems 2 and 3, written out explicitly:

Corollary 3. *Let*

$$\Delta_1 = d\left[\frac{2n(q-1) - (q-2)}{q} - d\right]$$

and

$$\Delta_2 = \frac{n(n-1)(q-1)^2}{q^2} - \frac{\Gamma^2}{n(n-1)q^2(q-1)^2},$$

where

$$\Gamma = (n-w)(n-w-1)(q-1)^2 - 2w(n-w)(q-1) + w(w-1).$$

If $\Delta_1 > \Delta_2$, *then*

$$B_q(n,d,w) \leqslant \frac{\Delta_1}{\Delta_1 - \Delta_2}.$$

Corollary 4. *If*

$$qd[2n(q-1) - (q-2) - qd] - (q-1)^2 n(n-1) > 0,$$

then

$$B_q(n,d) \leqslant \frac{qd[2n(q-1) - (q-2) - qd]}{qd[2n(q-1) - (q-2) - qd] - (q-1)^2 n(n-1)}.$$

The bound in Corollary 4 can also be obtained from the generalized Grey–Rankin bound derived by Fu, Kløve and Shen [6].

Example 1. For the case $n=q+1$, $d=q$, $w=q-1$ considered by Heise and Honold [9], $k=1$ gives the bound $q(q+1)/2$, $k=2$ gives the weaker bound q^2-1 and $k=3$ does not give a bound at all since (11) is not satisfied.

Example 2. If $d=((q-1)(n-1)+1)/q$, then

$$P_1(d)=q-2\geqslant 0$$

but

$$P_2(d)=-\frac{n(q-1)}{2}<0.$$

Hence Corollary 4 gives

$$B_q\left(n,\frac{(q-1)(n-1)+1}{q}\right)\leqslant 1+(n-1)(q-1).$$

Example 3. It is known that

$$B_q\left(\frac{q^r-1}{q-1},q^{r-1}\right)=q^r. \tag{13}$$

This can be shown using the Delsarte bound (1) and the existence of the simplex code.

If C is an $(n,M,d;q)$ equidistant code, then $C'=\{(0,c)\,|\,c\in C\}$ is an $(n+1,M,d;q)$ equidistant code. Hence

$$B_q(n+1,d)\geqslant B_q(n,d). \tag{14}$$

For $n=(q^r-1)/(q-1)+1$ and $d=q^{r-1}$ we have $d=((n-1)(q-1)+1)/q$. Hence, by Example 2, we have

$$B_q\left(\frac{q^r-1}{q-1}+1,q^{r-1}\right)\leqslant q^r. \tag{15}$$

Combining (13)–(15) we get

$$B_q\left(\frac{q^r-1}{q-1}+1,q^{r-1}\right)=q^r.$$

In contrast,

$$B_q\left(\frac{q^r-1}{q-1}-1,q^{r-1}\right)=q^{r-1}.$$

This follows from the Plotkin bound and a shortened simplex code.

Example 4. This example is to illustrate that in some cases we may have $P_k(d)<0$ only for large k. Let $d=2$. Then

$$B_q(3,2)=4 \quad \text{for } q\leqslant 4,$$

$$B_q(n,2)=\max\{n,q\} \quad \text{otherwise.}$$

An $(3,4,2;q)$ equidistant code is $\{(000),(110),(011),(101)\}$. The code consisting of the q code words $(\alpha,\alpha,0,\ldots,0)$ for all $\alpha\in GF(q)$ is an equidistant $(n,q,2;q)$ code. The code consisting of the code word $\mathbf{0}=(0,0,0,\ldots,0)$ and the $n-1$ code words $\mathbf{c}_i=(1,0\ldots,0,1,0,\ldots,0)$, for $i=2,3,\ldots,n$, (where the second 1 is in position i) is an equidistant $(n,n,2;q)$ code. It is easy to show that any maximal size code is equivalent to one of these codes.

We see that the Delsarte bound is sharp only in one case, namely when $n=3$ and $q=2$. Now consider the bounds in Theorem 3. We have

$$\frac{P_k(2)}{P_k(0)}=\frac{(n-k)(n-k-1)(q-1)^2-2k(n-k)(q-1)+k(k-1)}{n(n-1)(q-1)^2}.$$

This is negative only for k sufficiently large. More important, the value of k which minimizes $1-P_k(0)/P_k(2)$ is the value which minimizes $P_k(2)/P_k(0)$. It is easy to see that if we write

$$n=rq-s \quad \text{where } 0\leqslant s\leqslant q-1,$$

then the minimum is obtained for $k=n=r(q-1)-s$ (since k is integral). For this value of k, Theorem 3 gives the upper bound

$$1+(n-1)(q-1)-\frac{s(q-2-s)(n-1)(q-1)}{n(q-1)+s(q-2-s)}. \tag{16}$$

For $s=q-1$, this is exactly the Delsarte bound $1+n(q-1)$. However, for $s\leqslant q-2$, the bound is $\leqslant 1+(n-1)(q-1)$. We see that bound (16) is sharp for all q when $n=2$ and for all even n when $q=2$.

Acknowledgements

This research work is supported in part by the National Natural Science Foundation of China under the Grant 60172060, the Trans-Century Training Programme Foundation for the Talents by the Ministry of Education of China, the Research Grant Council of Hong Kong under Earmarked Grant CUHK 4424/99E, the DSTA project (POD 0103223), and the Norwegian Research Council.

The paper was presented at The International Workshop on Coding and Cryptography, held January 8–12, 2001, in Paris [5]. We thank the audience whose questions and other feedback have helped improve the presentation of the results of the paper.

References

[1] A.E. Brouwer, J.B. Shearer, N.J.A. Sloane, W.D. Smith, A new table of constant-weight codes, IEEE Trans. Inform. Theory 36 (1990) 1344–1380.

[2] P. Delsarte, Four fundamental parameters of a code and their combinatorial significance, Inform. and Control 23 (1973) 407–438.

[3] M. Deza, Une proprieté des planes projectifs finis dans une classe de codes equidistants, Discrete Math. 6 (1973) 343–352.

[4] F.-W. Fu, A.J. Han Vinck, S.-Y. Shen, On the constructions of constant-weight codes, IEEE Trans. Inform. Theory 44 (1998) 328–333.

[5] F.-W. Fu, T. Kløve, Y. Luo, V.K. Wei, On equidistant constant weight codes, in: D. Augot, C. Carlet (Eds.), Proceedings of the International Workshop on Coding and Cryptography, January 8–12, 2001, Paris, 2001, pp. 225–232.
[6] F.-W. Fu, T. Kløve, S.-Y. Shen, On the Hamming distance between two i.i.d. random n-tuples over a finite set, IEEE Trans. Inform. Theory 45 (1999) 803–807.
[7] J.I. Hall, Bounds for equidistant codes and partial projective planes, Discrete Math. 17 (1977) 85–94.
[8] J.I. Hall, A.J.E.M. Jansen, A.W.J. Kolen, J.H. van Lint, Equidistant codes with distance 12, Discrete Math. 17 (1977) 71–83.
[9] W. Heise, Th. Honold, Some equidistant constant weight codes, http://fatman.mathematik.tu-muenchen.de/ heise/MAT/code_oval.html.
[10] I. Heng, Ch. Cooke, Error correcting codes associated with complex Hadamard matrices, Appl. Math. Lett. 11 (4) (1998) 77–80.
[11] Y. Ionin, M.S. Shrikhande, Equidistant families of sets, Linear Algebra Appl. 226/228 (1995) 223–235.
[12] D.R. Stinson, G.H.J. van Rees, The equivalence of certain equidistant binary codes and symmetric BIBDs, Combinatorica 4 (1984) 357–362.
[13] M. Svanström, Ternary codes with weight constraints, Linköping Studies in Science and Technology, Dissertation No. 572, Department of Electrical Engineering, Linköping University, Sweden, 1999.
[14] J.H. van Lint, A theorem on equidistant codes, Discrete Math. 67 (1973) 353–358.
[15] J.H. van Lint, Introduction to Coding Theory, Springer, New York, 1982.
[16] V. Zinoviev, On the equivalence of certain constant weight codes and combinatorial designs, J. Statist. Plann. Inference 56 (2) (1996) 289–294.